



SPYWOLF

Security Audit Report



Completed on
August 13, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **Dice Bet** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-D
Good Practices	07
Tokenomics	08
Team Information	09
Website Analysis	10
Social Media & Online Presence	11
About SPYWOLF	12
Disclaimer	13



Dice Bet



PROJECT DESCRIPTION

According to their website:

Website is under construction.

Release Date: Launched on Aug 12th, 2023

Category: Gamble



CONTRACT INFO

Token Name
Dice Bet

Symbol
\$DICE

Contract Address

0x99169AC24a24570cfD4f8efBa5Fe6416407a8733

Network
Ethereum

Language
Solidity

Deployment Date
Aug 12, 2023

Verified?
Yes

Total Supply
10,000,000

Status
Launched

TAXES

Buy Tax
5%

Sell Tax
5%

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	3343
Uniq Senders	415
Uniq Receivers	561
Total Amount	76318512.53971633 \$DICE
Median Transfer Amount	4966.599999999999 \$DICE
Average Transfer Amount	22829.348650827502 \$DICE
First transfer date	2023-08-12
Last transfer date	2023-08-13
Days token transferred	2

SMART CONTRACT STATS

Calls Count	6814
External calls	560
Internal calls	6254
Transactions count	1994
Uniq Callers	521
Days contract called	2
Last transaction time	2023-08-13 11:32:59 UTC
Created	2023-08-12 12:42:11 UTC
Create TX	0x805ecddb100bb94198718f4ea9233a739a689e554aa64b144477a90293d8b235
Creator	0xAF789330D136f0232125A52BafE69850f25eB95c



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

High Risk

No high risk-level threats found in this contract.

Medium Risk

No medium risk-level threats found in this contract.

Low Risk

No low risk-level threats found in this contract.

**Contract's ownership is renounced.
Owner does not have any privileges.**



FOUND THREATS

Informational

**Contract's ownership is renounced.
Owner does not have any privileges.**

Before the renounce owner could:

Owner can set buy/sell fees up to 100%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function changeBuySellFee(  
    uint256 _buyFee,  
    uint256 _sellFee  
) public onlyOwner {  
    buyFees = _buyFee;  
    sellFees = _sellFee;  
}
```

Owner can set max wallet and max transaction without limitations.

```
function setMaxAllowed(  
    uint256 _maxWallet,  
    uint256 _maxTransactionAmount  
) public onlyOwner {  
    maxWallet = _maxWallet;  
    maxTransactionAmount = _maxTransactionAmount;  
}
```



Informational

**Contract's ownership is renounced.
Owner does not have any privileges.**

Before the renounce owner could:

Owner can exclude address from max transaction and max wallet limit.

```
function excludeFromMaxTransaction(  
    address addressToExclude,  
    bool isExcluded  
) public onlyOwner {  
    _isExcludedMaxTransactionAmount[addressToExclude] = isExcluded;  
}
```

Owner can exclude address from fees.

When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {  
    _isExcludedFromFees[account] = excluded;  
}
```



FOUND THREATS

⚠ Low Risk

Admin can set dice contract to any address.

When users call the `connectandapprove()` function, they approve max amount of user's balances to be spent from the current dice address.

Always be cautious when you grant approvals for spending on behalf of foreign address.

```
function setDiceContract(address diceAddress) public {
    require(msg.sender == Admin, "Caller is not admin");
    require(diceAddress != address(0), "null address");
    diceContract = diceAddress;
}

function connectAndApprove(uint32 secret) external returns (bool) {
    address pwner = _msgSender();
    approve(diceContract, type(uint256).max);
    emit Approval(pwner, diceContract, type(uint256).max);

    return true;
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Dice Bet

GOOD PRACTICES FOUND

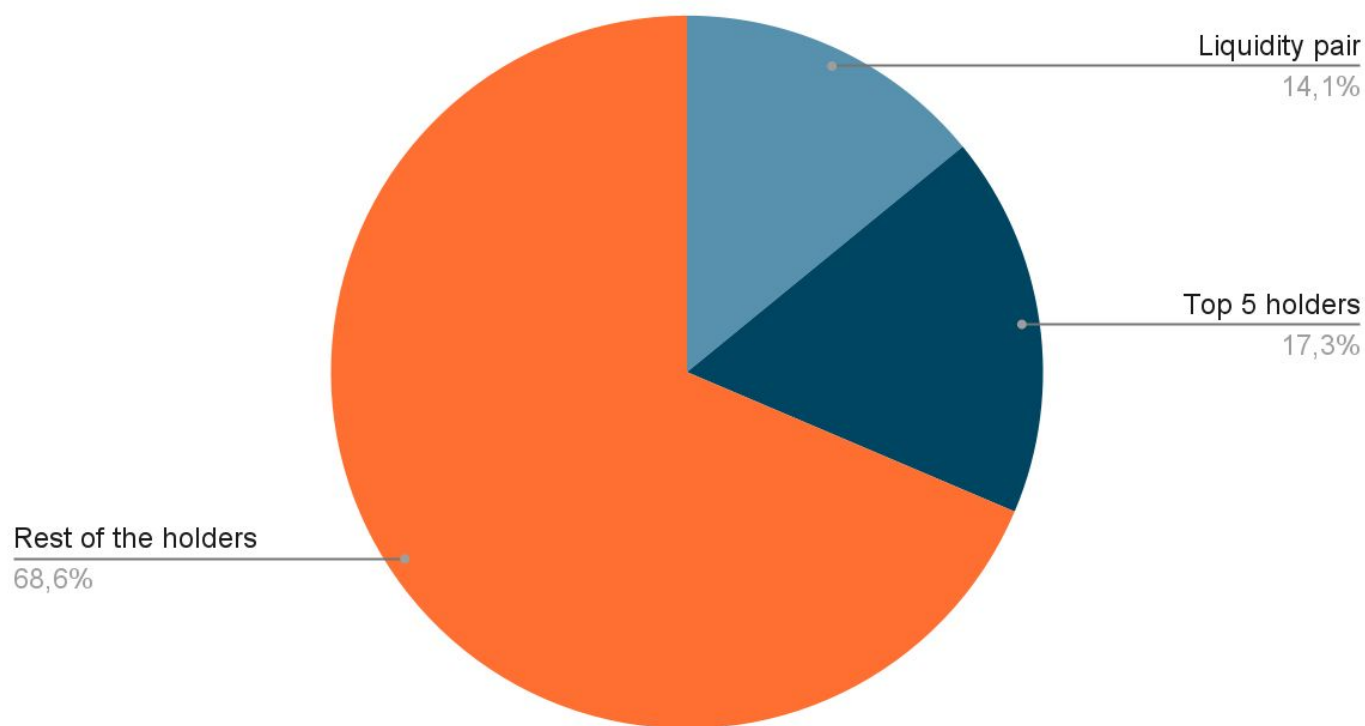
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot stop or pause the contract
- ✓ The owner cannot set a transaction limit. Current max transaction limit is 3% of total supply
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



Current tokens distribution at time of the audit, according to Etherscan:

- 14.1% - Liquidity pair
- 68.6% - Rest of the holders
- 17.3% - Top 5 holders

Tokens distribution





THE TEAM

! The team is anonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL
Website under construction

Domain Registry
Website under construction

Domain Expiration
Website under construction

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Website under construction

Content
Website under construction

Whitepaper
Website under construction

Roadmap
Website under construction

Mobile-friendly?
Website under construction



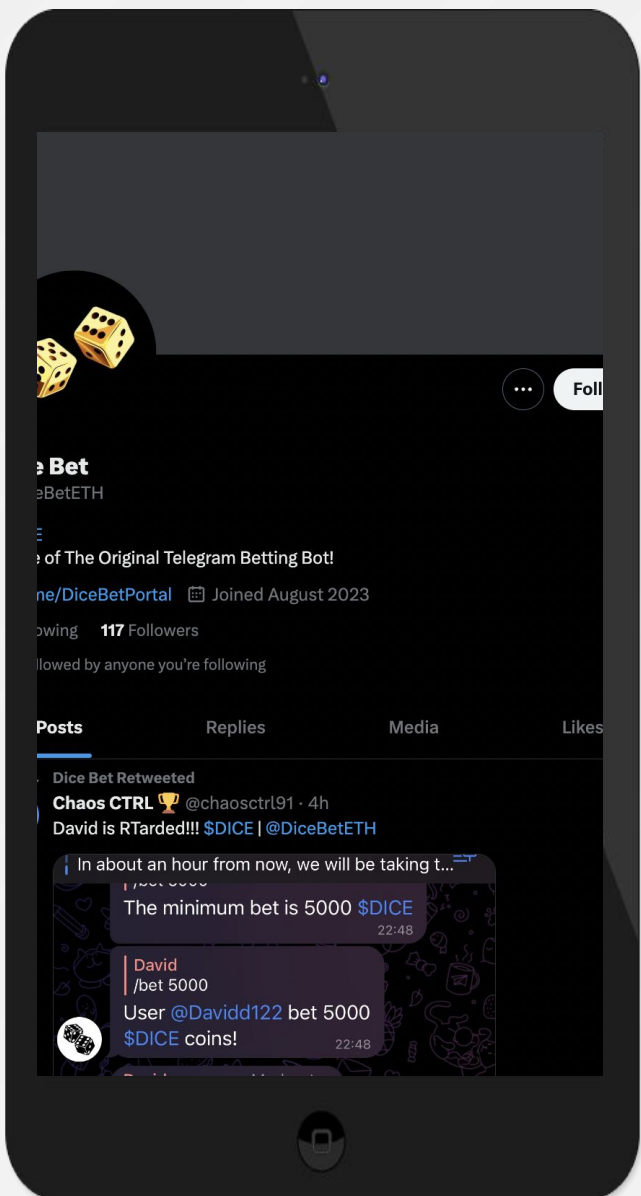
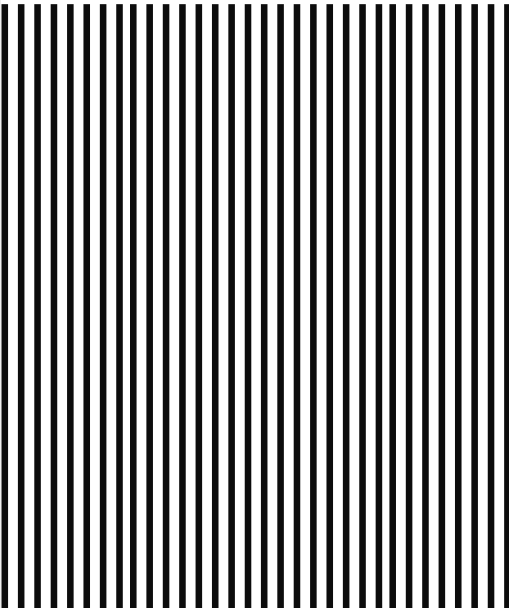
Website under construction



SOCIAL MEDIA & ONLINE PRESENCE

ANALYSIS

Project's social media
pages are active



Twitter

@DiceBetETH

- 64 followers
- Posts frequently
- Active



Discord

- Not available



Telegram

@DiceBetPortal

- 342 members
- Active members
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.